GESTÃO & PRODUÇÃO

ISSN 0104-530X (Print)
ISSN 1806-9649 (Online)

ORIGINAL ARTICLE

Organizational secrecy as viewed by the agents of a multinational corporation: A Case Study

Sigilo organizacional, visão dos agentes em uma corporação multinacional: Um estudo de caso.

Homero Cremm Busnelo[1], Julio Cesar Donadone[1]

[1] Universidade Federal de São Carlos – UFSCar, Departamento de Engenharia de Produção, Programa de Pós-graduação em Engenharia de Produção, Centro de Ciências Exatas e de Tecnologia, São Carlos, SP, Brasil. E-mail: homero.busnelo@gmail.com

How to cite: Busnelo, H. C. & Donadone, J. C. (2021). Organizational secrecy as viewed by the agents of a multinational corporation: A Case Study. *Gestão & Produção*, 28(1), e5700. https://doi.org/10.1590/1806-9649-2020v28e5700

Abstract: Only a limited number of theoretical studies have been conducted with regards to the issue of organizational secrecy. This study examines similar and different views about secrecy within three executive levels of an industrial multinational organization named *Motores.* This is achieved through a case study for which the data has been collected by using a survey-like questionnaire and semi-structured interviews. The different maturity levels and process structures in the enterprise account not only for different stages, concerns, and types of knowledge involved in addressing secrecy, but also for the role boundaries among the agents surveyed. Furthermore, while these agents are well acquainted with suppliers and customers, whereby confidentiality is ensured through confidentiality agreements (NDAs) and patent protection, their relationships with institutions and organizations appear to be areas of little or no knowledge, especially when it concerns competitors, class entities, and government relations. Leaks of classified information occur, and the places and situations where they may take place are identified. No potential mitigation situations were identified in our case study, and no systemic protocol exists for dealing with classified topics in the different areas where secrecy is involved, including business strategies. Transparency is recognized and desired; however, its risks and consequences require evaluation.

Keywords: Information **s**ecrecy; Transparency; Hierarchical view; Social process; Governance.

Resumo: Apenas um número limitado de estudos teóricos foram conduzidos sobre o estudo do sigilo organizacional. Esta pesquisa revela as semelhanças e diferentes visões dentro de uma organização multinacional industrial, foram pesquisados três níveis executivos e suas respectivas visões na empresa chamada *Motores.* É um estudo de caso com aplicação de uma pesquisa tipo survey e perguntas semi-estruturadas. Há diferentes níveis de maturidade e estrutura de processos dentro da *Motores* que demonstram haver diferentes estágios, preocupações e conhecimento sobre a temática do sigilo. Zonas de fronteira das áreas de atuação entre os agentes pesquisados foram observadas, as relações com fornecedores e clientes, os cuidados na temática do sigilo através de acordos de confidencialidade - NDA, patentes são bem conhecidos. As relações entre instituições e organizações, no entanto apresentam ser áreas de pouco ou nenhum conhecimento principalmente quando envolvem concorrentes, entidades de classe e relações governamentais. Vazamentos de informações

Received Oct. 13, 2019 - Accepted June 26, 2020
Financial support: None.

sigilosas existem e foram identificados locais e situações nos quais tais fatos podem ocorrer. Não foram identificadas situações de mitigação de potenciais vazamentos e nem a existência de um protocolo sistêmico na temática sobre assuntos classificados como sigilosos nas diferentes áreas que o tema está inserido, inclusive nas estratégias de negócios. A transparência é entendida e desejada, no entanto seus riscos e consequências precisam ser avaliados.

Palavras-chave: Sigilo da informação; Transparência; Visão hierárquica; Processo social; Governança.

1 Introduction

Human behavior may vary depending on the environmental factors that affect a particular individual's life, including whether family, educational institutions, workplace, or society. This theme has been the subject of various studies over time, in the different domains of anthropology, biology, biochemistry, philosophy, physiology, neurology, pedagogy, psychology, and sociology. Organizations have also been largely studied, and the most well-known types of organizations are state governments, corporations, political groups, armed forces, charities, service clubs, non-profits, cooperatives, educational institutions, religious institutions, and secret societies. There are also organizations that operate outside the legal system, which are classified as criminal organizations, gangs, terrorist groups, mobs, or the mafia. This study focuses on the actors who are immersed in organizations (Granovetter, 1985), their relationships between different hierarchical levels and peers (Fama & Jensen,1983), and also on the controls that must exist to prevent sensitive information, and secrets from leaking in intra-organizations or inter-organizations (Donaldson & Davis, 1991). According to Simmel (1906), people need to feel accepted when they become part of a group. Once accepted, the agent may start to receive information belonging to such a group. Depending on the level of trust the agent earns, the group may share the most secret information with this new member. Thus, the agent may learn about the "parallel" world that surrounds that organization.

Acceptance in the workplace is important for an individual to be a part of a particular organization, and this research focuses on a business organization that aims to understand an individual's behavior within a given organization through its different hierarchical levels and the relationships among peers and superiors. Possible external connections will also be examined in looking at inter-organizational relations between the studied company, competitors, suppliers, and institutions such as class entities and governmental entities from the perspective of information confidentiality and, where applicable, its antonym, transparency.

This research seeks to understand the arena of clash between the organization—its hierarchy, methods, processes, and internal and external relations—and the individuals (actors) its socio-economic interaction among peers, superiors, processes of integration and treatment of information, who are part of it. It is in this context and within the different existing groups that data and information demanding confidentiality resides; or it may take the opposite direction, which states that data or information should be made public, therefore transparent.

The works of Simmel (1906) and Goffman (1978, 2009) and more recently of Zerubavel (2006) may be some of the sources of reference for attaining a better understanding of how secrets are understood, maintained and controlled by the agents.

Problems and consequences related to intentional concealment have also been studied by Bok (1989).

Trust in relationships in organizations are of great importance, especially considering the fact that the individual is partly or, more often, totally absorbed by the embeddedness effect within the organization. According to Granovetter's (1985, p. 53) definition, embeddedness is, "the argument that behavior and the institutions to be analyzed are so limited by the ongoing social relations that to construe them as independent is a grievous misunderstanding."

Privacy as a right, property laws, and boundaries between private and public life were discussed by Warren & Brandeis (1890), with reference to the technological revolution of the late 19th and early 20th centuries, when the advent of photography began to expose images of social life that was hitherto kept private. Nowadays, there is equal or an even greater pressure on property rights over digital content.

Regarding behavior, Costas & Grey (2014) studied organizational secrecy as a social process and shed light on the formal and informal concealment of information maintained by agents within a given organization. This study goes one step further in terms of the agent´s understanding of secrecy, the relations with organization processes and interaction that involves different aspects of daily life in a business organization. This research also complements the study by Zucker et al. (1994), which analyzes the impact of leaks that occur in the biotechnology industry and spread knowledge among surrounding companies. The findings of this study lie in the fact that it brings to the surface the agents' view of secrecy, the impacts on transparency and deficiencies in the agency's control (Donaldson & Davis, 1991). Trust is seen as important for the performance of organizations. As shown below there are boundaries, which despite their commitment to the organization, the agents present a lack of understanding and knowledge about what can be revealed, shared and what are the different iterations that occur in the external environments that comprise an organization, their economic interests and immersion problems (Granovetter, 1985).

Documents have been stolen via electronic media from the archives of home computers of citizens and from large organizations, exemplified by the case of state secrecy defined by Habermas & Habermas (1991), Marin (1998) and Horn (2011). Recent examples include the US Government data leakage (in the case known as WikiLeaks, cited in Lafer (2011); the theft of equipment and documents containing important information about the Brazilian Petrobras multinational in the petroleum business (G1, 2008); and millions of documents from the NSA that were stolen by a CIA employee, in the Edward Snowden case (The Economist, 2013).

In the entertainment area, the Disney film "Pirates of the Caribbean" was stolen by hackers demanding a ransom in Bitcoin, which, according to the Disney CEO, would not be paid (Yu & Weise, 2017). In the same article, the authors also included a brief note about the Sony hacking case in 2004, when terabytes of private corporate data were hacked and leaked to the public. In this case, it was suspected as an attack backed by North Korea, as Sony was about to launch a comedy depicting the assassination of the country's leader, Kim Jong Un.

Many other cases could be included here, but what should be taken into consideration in the examples presented above are the issues related to organizations and their actors. This study does not intend to propose security architecture in operating systems, but rather present the views regarding the issue from the perspective of an organization's executives at three levels: top, middle, and operational. This case study reveals where the boundaries of information secrecy are and their impact on

transparency, from the point of view of agents at different hierarchical levels in a large organization.

2 Theoretical framework

A specific theory dealing with the issue of confidentiality in organizations is yet to be written, according to Grey & Costas (2016), insofar as

> It is woven into the fabric of all organizations in a multitude of ways [...] the broadly conceived understanding of organizational secrecy perhaps accounts for the paradoxical nature of attempting to study it (Grey & Costas, 2016, p. 1).

Furthermore, secrecy can be found in different areas of human knowledge and the following sources of information can be mentioned as the most relevant to its study:

i) The sociological perspective of secrecy is addressed by Georg Simmel, who sees it as a cornerstone in understanding the conscious and unconscious evolution of the mind, the possibility of a second world parallel to the known obvious world (1906).

ii) Secrecy can also be seen as a complex social process (Goffman, 1978, 2009; Zerubavel, 2006; Costas & Grey, 2014).

iii) Bureaucracy and hierarchy are approached in the studies of Fama & Jensen (1983), March & Simon (1958), Weber (2013).

iv) Trust, the reference base for institutionalization, is a construct ensured by studies focused on inter-organizational cooperation and its relations (Arnott, 2007; Grandori & Soda, 1995; Rao & Schmidt, 1998; Zaheer & Harris, 2006; Currall & Inkpen, 2002; Ferrin et al., 2006. Kroeger, 2012) addressed the mechanisms and processes of the institutionalization of trust at individual and interorganizational levels.

v) Corporate governance and strategy are approached by Capasso & Dagnino (2014). This current study makes use of a finding of their case that corporate governance can prevail over strategic management at times, rather than strategic management over corporate governance. The vast literature on governance includes Jensen and Meckling (1976), Williamson (1984), Jensen & Warner (1988), Hart & Moore (1990), Roe (1994), Denis (2001), Charreaux & Desbrières (2001) and Jensen (2002).

vi) Corporate strategy is referenced in Porter (2008), Rumelt et al. (1995), Teece (1988), Teece et al. (1997), Harrigan (2003), Barca (2017), Bromiley (2005), Capasso et al. (2005), Hoskisson et al. (2004), Barney (2006).

vii) The virtue of secrecy as an important asset is addressed by Dufresne & Offstein (2008).

viii) Human capital as any another important asset, in this case, a mobile asset, is seen in Coff (1997) and, more recently, in Hannah (2007).

ix) Written and unwritten information was studied by Thompson & Kaarst-Brown (2005) and March et al. (2000) giving relevance to how external influences within organizations affect their internal processes.

x) Busnelo & Donadone (2019) (unpublished manuscript) have identified three pillars that support secrecy composed of elements of the organization and their intra and

inter organizational relationships. The environment in which the business is inserted is influenced at the micro or macro level and the human part that involves the actors (agents) and their mobility associated with the information topic are potential elements and sources of risk of leakage for preserving confidential information.

xi) Ku (1998) analyzed the cultural and political influences of the public sphere versus the practice of open/secret politics by the state. Although the state is expected to be transparent and public, it is also expected that information classified as sensitive remains under controlled secrecy, even though leaks may occur.

xii) Robert Merton deconstructs the study of secrecy when applied to scientific works. It simply does not exist, as presented by Vermeir & Margócsy (2012) in their historiographical study on the scientific study of secrecy.

xiii) Eva Horn (2011) rescues the concepts of the Latin terms *mysterium*, *arcanum* and *secretum* to describe the dimensions of secrecy in her study about the logics of political secrecy

xiv) Derrida et al. (1994) discuss secrets supposed to be known that are excluded from knowledge and excluded from revelation

xv) Galison (2004) analyzes classified official and military documents as well as how to remove knowledge

xvi) business secrets involving customer lists, business plans, or manufacturing processes are not protected by law as set forth in Friedman et al. (1991)

xvii) the management of intellectual property is addressed by Delerue & Lejeune (2011)

xviii) Stohl & Stohl (2011) address the metaconversations of clandestine organizations and secret agencies as a tool that helps to better understanding their behavior.

The aforementioned literature presents different aspects of secrecy in society, in organizations, and political environments but does not represent it from the point of view of the agent. The way secrecy is understood and when transparency is recommended from the perspective of the agents are aspects that still need to be investigated. This study brings some of these agent views to light. Some studies can be mentioned because they are more oriented from the perspective of agents, such as Zucker et al. (1994), in which the intellectual capital is represented by renowned scientists. Here they can be classified as L1, since only the executive level has been studied. Hierarchy levels were studied by Diefenbach & Sillince (2011) from the perspective of formal or informal types and its differentiation, more oriented on organization structure as a consequence and driven to understand the organization management. The study carried out by Hannah (2007) analyzed the behavioral factors that influenced new employees or, in other words, understand how they protect or share the secrets of the organization for which they worked beforehand, emphasizes individuals in transition and possible feelings of obligation with their former employers and the new social group in which they are newly inserted (Hannah, 2007). What is new in the present study is that the agents interviewed are not new, they have worked for years in the same organization, and the questions asked were guided towards the agent's understanding of secrecy, when it reveals it, its ownership and consequences. On the other hand, Hannah (2007) researched agents in transition, recently arrived at two high-tech companies. This study aimed to find out the influence of belonging to a group as employees tend to act in favor of their new employer (Hannah, 2007). It is

important to highlight that the study carried out by Hannah does not classify the results obtained in hierarchical levels, differently from the one presented in the present study. The interviewees are classified in three hierarchical levels: L1; L2; and L3. This categorization clarifies the different influences that secrecy can bring to the preservation, disclosure or leakage of confidential information in intra or inter organizations. This study covers hierarchical, process control, decision measures related to inter-organization relations, agent behavior related to secrecy concern, trade secrecy, information sharing, hacking, patent and technological development in one given organization, henceforth called MOTORES.

The methods adopted for the survey research and semi-structured interviews at *Motores* are presented next.

3 Research method and research question

The research plan is to conduct the analysis of a large company regarding our subject at hand. The company's size can be defined by various criteria, such as revenue, market share, number of employees, according to MacCarthy & Fernandes (2000). However, the definition of "large" for companies can also vary among countries. For instance, whereas in the UK, a company is large if it employs more than 250 employees, in Brazil the number of employees should exceed 500. The company considered in this research has over 1,000 employees, and therefore is considered large. It is located in Brazil and is a multinational.

Another reason for analyzing large companies is that they are managed by compliance systems, their results are audited, they often stock market shares, and they follow local laws —such as Law No. 12,529 on antitrust Brasil (2011)—and compliance laws in the USA—USA, SOX, OFAC. These laws and market positioning suggest that the handling of information and the views of its actors on its content are known, disseminated within the organizational structure and permeate decision-making in micro intraorganizational and macro intergoranizational environments.

The organization chosen will be simply referred to as *Motores* here, for the sake of preserving its identity. This multinational has operated in Brazil for many years, its products reach the national and international markets, and it conducts business-to-business transactions.

A survey was designed and applied to three levels of the organization: L1 represents the senior executive level, L2 the middle management and L3 the low management level. By and large, L1 is positioned in an environment where strategic decisions dominate much of the agenda, L2 where tactical decisions are made, and L3 mostly in charge of tactical/operational issues.

This study proposes that convergent and divergent views among the actors involved should be identified. The questionnaire devised contains a Likert scale of response categories 1 to 5 (Bertram 2007), where 1 represents lack of agreement and 5 complete agreement. Category 6 was also made available, characterizing the respondent's total ignorance about the topic. This option was used to identify possible frontiers of knowledge, i.e., the areas less dominated by the sample of the studied population (in this case, N = 76). The questions and statement of the survey are listed below:

1- Is there information in my area that has restricted access and is determined by: written procedures; verbal instructions or is there no guidance?

2- In the case of access violation, in the event of information leakage, is there a containment plan based on: written procedures; verbal instructions or is there no guidance?

3- Do guidance, monitoring and communication measures apply to people who have responsibilities and strategic positions when handling sensitive data for the organization?

4- When an employee who has access to sensitive organization data is dismissed, is there an interview procedure that emphasizes that he/she must keep such information confidential even if he/she is moving to another company, including a competitor?

5- I make decisions only with the consent of my superiors, in the following situations: in matters related to suppliers; related to customers; related to competitors; related to class entities and related to government issues.

6- How do you rate your daily concern in preserving certain sensitive information for the company, in which you work, away from the market? Related to suppliers; related to customers; related to competitors; related to class entities and related to the government.

7- Should the data on the company's business be known to all employees?

8- If companies have a problem, should it be shared with everyone?

9- Are there written procedures that ensure compliance with the strategic plan to make the organization more competitive and ensure that leaks do not occur?

10- Regarding sharing information from your previous company: Would you share strategic information from your previous employer if this information is requested by your current employer?

11- Should the company be careful when controlling and disclosing data about a new product so that such information is not obtained by hackers?

12- Does the company I work for take this type of care?

13- Does a product's patent ensure protection against competitors' actions?

14- Can the company develop technology in its research centers or even seek developments through cooperation programs with universities or open science? Do you believe in technological development made with your own resources?

A triangulation was generated through the case study. The actors of L1, L2, and L3 were interviewed individually through semi-structured interviews. The following questions were asked:

i. How do you understand confidentiality?

ii. Why does confidentiality exist?

iii. When should confidentiality be revealed, to whom, and why?

iv. What should not be revealed and why not?

v. Is transparency required? When or under what circumstances is it required?

The semi-structured interview technique was used within the corporate environment, thus leading to an immersion study, with embedded units. This is therefore a unique case study (Yin, 2009).

The study seeks answers to how organizational secrecy is viewed by the organization’s actors. Some possible points of clarification may lead to a better understanding of the formal and informal types of confidentiality rules,

coverage/influence areas and boundaries where such information or knowledge is limited or diffused.

The survey questionnaire was e-mailed to the target audience after authorization granted by *Motores* management, see Table 1. All the agents involved were previously informed about the survey, as well as the fact that it was voluntary and that the identity of the respondents would be preserved. The survey and semi-structured interviews took place between spring and summer 2017/18, totaling approximately 6 months.

The results obtained from this article are limited by the studied environment and its actors. Moreover, it is possible to infer analogies with other organizations that this must be done carefully, even in similar segments, size and geographic scope.

Our findings refer solely and exclusively to *Motores* and its actors within the period in which the research was conducted.

The data collected through the survey has been analyzed based on the percentage of responses per group of respondents L1, L2 and L3. Concomitantly, the responses were analyzed together in the form of descriptive statistics (Bertram, 2007) informing mode, median, response range and interquartile range.

The semi-structured interviews were not recorded in order to avoid inhibiting openness from the respondents. Sessions lasted from 30 to 60 minutes, in which twenty-one professionals were interviewed; six L1, six L2, eight L3, and one L3 who answered only questions 1 and 2, which were incorporated into the analysis.

4 Research findings based on the survey data (Table 1)

Table 1 shows that restricted access to sensitive information either as written procedures or verbal guidance did not present a definite position since inter-quartiles for both written procedures indicate scale 3, and for verbal guidance scale 2; in both cases, the dispersion is significant because its scale is 4.

Table 1. L1: Senior executive level; L2: Middle management level; L3 Low management level.

Quest. nr.	Likert Scale ->	Total Partic.	Unit	No coverage (1)			A small portion (2)			With some coverage (3)			Moderate coverage (4)			Great coverage (5)			Mode	Median	Range	Inter-quartile Range
	Hierarchy Level ->	n		L1	L2	L3	L1	L2	L3	L1	L2	L3	L1	L2	L3	L1	L2	L3				
1	There is information in my area that has restricted access and this is determined by:																					
1a	Written procedures	28.0	#	1.0	3.0	2.0	1.0	4.0	2.0	0.0	1.0	1.0	0.0	1.0	4.0	2.0	1.0	5.0	2	3	4	3
			%	25.0	30.0	14.3	25.0	40.0	14.3	0.0	10.0	7.1	0.0	10.0	28.6	50.0	10.0	35.7				
1b	Verbal instructions	29.0	#	0.0	3.0	1.0	2.0	2.0	5.0	1.0	2.0	3.0	1.0	3.0	1.0	0.0	0.0	5.0	2	3	4	2
			%	0.0	30.0	6.7	50.0	20.0	33.3	25.0	20.0	20.0	25.0	30.0	6.7	0.0	0.0	33.3				
1c	There is no orientation	17.0	#	3.0	3.0	2.0	0.0	2.0	5.0	1.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	1	1.5	2	1
			%	75.0	60.0	25.0	0.0	40.0	62.5	25.0	0.0	12.5	0.0	0.0	0.0	0.0	0.0	0.0				
2	In case of violation of this access, when information leakage occurs, there is a containment plan:																					
2a	Written procedures	15.0	#	2.0	3.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0	1.0	4.0	1	1	4	4
			%	50.0	75.0	42.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	50.0	25.0	57.1				
2b	Verbal instructions	16.0	#	1.0	1.0	3.0	2.0	0.0	2.0	1.0	2.0	1.0	0.0	0.0	0.0	0.0	1.0	2.0	1	2	4	2
			%	25.0	25.0	37.5	50.0	0.0	25.0	25.0	50.0	12.5	0.0	0.0	0.0	0.0	25.0	25.0				
2c	There is no orientation	14.0	#	3.0	2.0	4.0	0.0	1.0	4.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1	1	1	1
			%	100.0	66.7	50.0	0.0	33.3	50.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0				
3	Guidance, monitoring and communication measures are applied to people who have a strategic position and responsibility in dealing with data sensitive to the organization.	28.0	#	0.0	0.0	1.0	1.0	4.0	3.0	0.0	3.0	3.0	1.0	2.0	3.0	2.0	1.0	4.0	2	3	4	2.5
			%	0.0	0.0	7.1	25.0	40.0	21.4	0.0	30.0	21.4	25.0	20.0	21.4	50.0	10.0	28.6				
4	When an employee who has access to sensitive data of the organization is dismissed, an interview is given, emphasizing that he / she must keep such information	8.0	#	0.0	1.0	1.0	0.0	0.0	0.0	1.0	1.0	2.0	0.0	0.0	0.0	0.0	1.0	1.0	3	3	4	2

Quest. nr.	Likert Scale ->	Total Partic.	Unit	No coverage (1)			A small portion (2)			With some coverage (3)			Moderate coverage (4)			Great coverage (5)			Mode	Median	Range	Inter-quartile Range
	Hierarchy Level ->	n		L1	L2	L3	L1	L2	L3	L1	L2	L3	L1	L2	L3	L1	L2	L3				
	confidential even when he or she is on the way to another company, including a competitor.																					
			%	0.0	33.3	25.0	0.0	0.0	0.0	100.0	33.3	50.0	0.0	0.0	0.0	0.0	33.3	25.0				
5	I make decisions only under the consent of my superiors, for each of the following situations:																					
5a	In subjects related to suppliers	29.0	#	0.0	1.0	1.0	1.0	2.0	1.0	1.0	2.0	1.0	0.0	1.0	2.0	1.0	3.0	12.0	5	5	4	2
			%	0.0	11.1	5.9	33.3	22.2	5.9	33.3	22.2	5.9	0.0	11.1	11.8	33.3	33.3	70.6				
5b	In subjects related to customers	32.0	#	0.0	0.0	3.0	0.0	0.0	0.0	1.0	3.0	2.0	1.0	3.0	1.0	2.0	5.0	11.0	5	5	4	2
			%	0.0	0.0	17.6	0.0	0.0	0.0	25.0	27.3	11.8	25.0	27.3	5.9	50.0	45.5	64.7				
5c	In subjects related to competitors	22.0	#	0.0	0.0	3.0	0.0	0.0	0.0	0.0	2.0	1.0	0.0	1.0	2.0	3.0	4.0	6.0	5	5	4	2
			%	0.0	0.0	25.0	0.0	0.0	0.0	0.0	28.6	8.3	0.0	14.3	16.7	100.0	57.1	50.0				
5de	In subjects related to class associations	25.0	#	0.0	0.0	4.0	0.0	1.0	0.0	0.0	3.0	1.0	1.0	0.0	1.0	1.0	4.0	9.0	5	5	4	2
			%	0.0	0.0	26.7	0.0	12.5	0.0	0.0	37.5	6.7	50.0	0.0	6.7	50.0	50.0	60.0				
5e	In subjects related to government	22.0	#	0.0	1.0	5.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0	0.0	1.0	1.0	6.0	7.0	5	5	4	4
			%	0.0	14.3	38.5	0.0	0.0	0.0	0.0	0.0	0.0	50.0	0.0	7.7	50.0	85.7	53.8				
6	How do you rate your daily concern about preserving certain sensitive information for the company, where you work, away from the market?																					
6a	In subjects related to suppliers	29.0	#	0.0	0.0	0.0	0.0	0.0	0.0	1.0	1.0	0.0	1.0	0.0	3.0	2.0	8.0	13.0	5	5	2	0
			%	0.0	0.0	0.0	0.0	0.0	0.0	25.0	11.1	0.0	25.0	0.0	18.8	50.0	88.9	81.3				
6b	In subjects related to customers	30.0	#	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0	3.0	9.0	16.0	5	5	3	0
			%	0.0	0.0	0.0	0.0	10.0	0.0	0.0	0.0	0.0	25.0	0.0	0.0	75.0	90.0	100.0				
6c	In subjects related to competitors	26.0	#	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0	0.0	1.0	2.0	9.0	12.0	5	5	1	0
			%	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	50.0	0.0	7.7	50.0	100.0	92.3				

Quest. nr.	Likert Scale ->	Total Partic.	Unit	No coverage (1)			A small portion (2)			With some coverage (3)			Moderate coverage (4)			Great coverage (5)			Mode	Median	Range	Inter-quartile Range
	Hierarchy Level ->	n		L1	L2	L3	L1	L2	L3	L1	L2	L3	L1	L2	L3	L1	L2	L3				
6de	In subjects related to class associations	23.0	#	0.0	0.0	1.0	1.0	0.0	0.0	0.0	0.0	0.0	1.0	0.0	2.0	1.0	7.0	10.0	5	5	4	0.5
			%	0.0	0.0	7.7	33.3	0.0	0.0	0.0	0.0	0.0	33.3	0.0	15.4	33.3	100.0	76.9				
Quest. nr.	Likert Scale ->	Total Partic.	Unit	No coverage (1)			A small portion (2)			With some coverage (3)			Moderate coverage (4)			Great coverage (5)			Mode	Median	Range	Inter-quartile Range
6e	In subjects related to government	22.0	#	0.0	0.0	0.0	1.0	1.0	0.0	0.0	0.0	1.0	1.0	0.0	0.0	1.0	6.0	11.0	0	0	0	0
			%	0.0	0.0	0.0	33.3	14.3	0.0	0.0	0.0	8.3	33.3	0.0	0.0	33.3	85.7	91.7				
7	Company's business data must be known by all employees.	32.0	#	0.0	1.0	2.0	0.0	1.0	3.0	1.0	0.0	2.0	2.0	7.0	6.0	1.0	1.0	5.0	4	4	4	1
			%	0.0	10.0	11.1	0.0	10.0	16.7	25.0	0.0	11.1	50.0	70.0	33.3	25.0	10.0	27.8				
8	If the company has a problem the same should be shared with everyone?	32.0	#	0.0	2.0	2.0	0.0	2.0	2.0	1.0	0.0	0.0	2.0	5.0	11.0	1.0	1.0	3.0	4	4	4	1.5
			%	0.0	20.0	11.1	0.0	20.0	11.1	25.0	0.0	0.0	50.0	50.0	61.1	25.0	10.0	16.7				
9	Are there written procedures that ensure compliance with the strategic plans to make the company more competitive ensuring that leaks don't happen?	27.0	#	0.0	0.0	0.0	0.0	0.0	2.0	0.0	1.0	2.0	3.0	3.0	2.0	1.0	6.0	7.0	5	5	3	1
			%	0.0	0.0	0.0	0.0	0.0	15.4	0.0	10.0	15.4	75.0	30.0	15.4	25.0	60.0	53.8				
10	About sharing information from your past company:																					
10a	Would you share strategic information from your previous employer if this information is requested by your current employer?	30.0	#	3.0	5.0	11.0	1.0	2.0	1.0	0.0	1.0	2.0	0.0	1.0	2.0	0.0	0.0	1.0	1	1	4	1
			%	75.0	55.6	64.7	25.0	22.2	5.9	0.0	11.1	11.8	0.0	11.1	11.8	0.0	0.0	5.9				
11	The company must take care of the control and disclosure of data about a new product, in order to avoid the abduction of	30.0	#	0.0	0.0	1.0	0.0	1.0	2.0	0.0	0.0	1.0	1.0	0.0	2.0	3.0	8.0	11.0	5	5	4	1

Quest. nr.	Likert Scale ->	Total Partic.	Unit	No coverage (1)			A small portion (2)			With some coverage (3)			Moderate coverage (4)			Great coverage (5)			Mode	Median	Range	Inter-quartile Range
	Hierarchy Level ->	n		L1	L2	L3	L1	L2	L3	L1	L2	L3	L1	L2	L3	L1	L2	L3				
	information by hackers.																					
			%	0.0	0.0	5.9	0.0	11.1	11.8	0.0	0.0	5.9	25.0	0.0	11.8	75.0	88.9	64.7				
12	**The company where I work takes this type of care.**	15.0	#	0.0	0.0	0.0	1.0	0.0	1.0	2.0	0.0	1.0	1.0	2.0	2.0	0.0	2.0	3.0	4 and 5	4	3	2
			%	0.0	0.0	0.0	25.0	0.0	14.3	50.0	0.0	14.3	25.0	50.0	28.6	0.0	50.0	42.9				
13	**The patent on a product ensures protection against copy actions by competitors.**	28.0	#	0.0	0.0	1.0	0.0	0.0	1.0	3.0	4.0	1.0	0.0	0.0	5.0	1.0	6.0	6.0	5	4	4	2
			%	0.0	0.0	7.1	0.0	0.0	7.1	75.0	40.0	7.1	0.0	0.0	35.7	25.0	60.0	42.9				
14	**The company can develop technology in its research centres or even seek to develop the through programs of cooperation with universities or open-science. Do you believe in technological development carried out with your own resources?**	30.0	#	0.0	0.0	0.0	0.0	1.0	1.0	1.0	2.0	5.0	2.0	5.0	9.0	1.0	1.0	2.0	4	4	3	1
			%	0.0	0.0	0.0	0.0	11.1	5.9	25.0	22.2	29.4	50.0	55.6	52.9	25.0	11.1	11.8				

Note: Authors´ own work.

These numbers indicate a dispersion of opinions regarding the existence of information restriction guidelines in the survey respondents' area of expertise. While analyzing the same issue with the statement that there is no guidance on restricted information in their area of activity, two factors come to light: there was a significant decrease in interquartile variation, in this case 1; both mode and median fell by half compared to the two previous conditions, of 2 to 1 and 3 to 1.5 respectively, as did the range, which decreased from 4 to 2.

The second factor that emerges from the analysis concerns the high number of respondents who rated such a condition as "unknown". Restricted access to sensitive information, therefore, shows homogeneity for those who responded within the Likert scale that there are written and verbal orientations, despite the different levels of clarity. Regarding the violation of restricted information or the existence of leaks, the focus was to know whether there were written or verbal guidelines or not. Respondents indicated that there are no written procedures to guide which measures to mitigate a given leak should be taken. When analyzing the mode and median, however, the range and the interquartile range presented the maximum degree, 4.

There are therefore opposing views among the interviewed agents. Whether one group agrees that mitigation actions are written, the other denies such existence, with a dispersed distribution curve. There may be different structures here depending on the area being evaluated, but unfortunately this detail is not within the scope of this research. The absence of verbal guidelines for leakage mitigation has mode 1 and median 2; once more the range is maximum, 4, as in the case of written guidelines. The interquartile is, however, reduced by half, indicating a shift of views, in favor of the condition of not having any verbal guidance in case of information leakage or access violation. Only one agent interviewed by the semi-structured method admitted that there had been leakage of sensitive information in *Motores* in the past.

Divergent views may stem from ignorance or even fear of answering this question. Another point reinforcing the lack of knowledge about leaks regarding the existence of written procedures or verbal orientations originates from the high rate of respondents who reported not knowing such conditions. A frontier for the unknown emerged, 50% of which lacked written instructions, 42.8% of which lacked verbal guidance and 48.1% of which lacked such instructions.

A communication and guidance system to preserve the organization's confidential and sensitive information has not been confirmed, but a non-disclosure contract can be signed, from the view of the company's agents. It is applied under special conditions for disclosing information about new projects when they need to be shared with other organizations, which is the most significant feature in the areas of research and development, legal and human resources. Only one agent confirmed the use of this resource, representing only 3, 1% of respondents.

The organization must establish confidentiality protocols and boundaries for its agents, having defined the form and operational procedure for those who have access to confidential information. Guidance, monitoring and communication measures were identified by respondents according to mode = 2. In cases of low occurrence, low frequency for the existence of such procedures and controls, the median moved more to the center, allowing us to conclude that due to this and to the range = 4, there is a diffusion of procedures, thus leading to the understanding that there is no central, formal and systematic structure present.

This permeable structure became evident with the analysis of the answers to the question about the measures adopted and care taken at the dismissal of an employee

who during his or her period of work in the organization had access to sensitive data. A significant portion of respondents (75%) indicated not knowing any rules about this procedure, even analyzing the actors who responded within the Likert scale signaling that there is no such procedure systemically, once there is dispersion in responses obtained with mode and median equal to 3, range to 4 and interquartile equal to 2.

In other words, when leaving the organization's agents who had access to company data, they are not reminded of their responsibilities for protecting confidential information, not sharing it with their new employer. However, agents should have an understanding of sensitive company issues and recognize the boundaries of micro and macro environments (Busnelo & Donadone, 2019). These are relevant points in the use and handling of strategic and tactical information involving ongoing business, future investments, acquisitions, mergers or even in launching new products or services.

The limits in which such decisions are made by agents were evaluated considering the degree of hierarchical dependence or their autonomy within the environment where they are inserted. The extant organizational structure in *Motores* is hierarchical whereby decisions are made only with the consent of superiors in the following areas: matters related to suppliers, customers, competitors, class entities and when involving the government. Mode and median were 5 in all areas considered and a range of 4, only highlighting the interquartile of 4 for government-related issues. This led to the evaluation of the incidence of non-respondents in this question, that is, for the survey respondents who stated they did not know about the existence of a hierarchy of authorization to deal with certain subjects, in which themes involving competitors, class associations and government were emphasized.

It is evident that there is greater mastery, hierarchical knowledge when dealing with issues related to suppliers and customers as they are part of a daily agenda in the daily activities of agents. On the contrary, matters related to competitors, class entities and government are more distant and can be said to be in an orbit farther from the command and control nucleus of the hierarchical structure, signaling a lack of knowledge of a significant portion of the agents, 31.3%. They are unaware of this structure when the issue involves competitors, 21.9% when it involves class entities and 31.3% when it involves government issues.

These three spheres of relationship between organizations and institutions are on the unknown frontier of most executive agents, thereby subjecting the issues surrounding them to risks of unintentional leakage. This may occur because mainly the agents classified here as L1 and L2 participate in these environments and are susceptible to exposure situations of sensitive topics that may occur objectively or subjectively within agendas other than a specific theme related to sensitive information that should remain confidential.

Continuing on the issue of routines, now focused on daily activities in matters of confidentiality, the survey also asked the agents what level of daily concern they had with preserving certain sensitive information that belongs to the organization in which they work. The objective here is to maintain sensitive information away from the market, and this question also confers the degree of adherence regarding contacts with suppliers, customers, competitors, class entities and government relations.

The answers converged, presenting less dispersion than in the previous question, that is, the agents have daily concerns about maintaining confidentiality insofar as the results presented a mode and median equal to 5, a range equal to 2 for suppliers and 1 for competitors, and interquartile zero for all three of these spheres of relationships.

The spheres of customer relations, class associations and government relations are in the opposite direction, although they presented a mode and median equal to 5. These show a greater dispersion of views; the range is 3 for customers, 4 for class entities and 3 for government. Interquartile results ranged from 0 to 0.5 for these last three spheres.

It can be concluded that the issues related to the daily concerns of agents in preserving confidential market information are more strongly related to the spheres of suppliers and competitors, while the spheres of customers, class entities and government are more distant.

It can be inferred in the case of class and government entities that such distancing may be explained by the lower frequency of these daily contacts than others. Customer relations, however, cannot be explained by the low frequency of daily contacts, suggesting that there is another possible factor, unidentified by the present study. Complementing this analysis is a view on the agents that have not answered this question because they classified it as ignoring the subject. The largest absences were in the issues related to competitors, class entities and government, respectively, 18.8%, 28.1% and 31.3%.

The survey asked respondents whether the organization's business data should be known to all members of the organization. The mode and median indicated that yes, 4, the vast majority of information must be known to all its members. However, the range demonstrated that there is an important dispersion of opinions. Despite being in smaller number, agents indicated that not everything should be transparent, suggesting that certain topics should be given special treatment. The survey does not allow a better understanding in this aspect. The agents could be concerned about commenting on issues regarding business strategy, some financial and labor results, processes, research projects and also actions for business expansion in certain regions.

Another point that draws attention, in this question, is that no respondent stated not knowing about the subject, that is, the surveyed population had a definite opinion, either for or against transparency or confidentiality. The subjective field that emerged in the previous questions disappeared; agents had an opinion which may differ more in favor of one over the other topic.

Following the same reasoning as the previous question, should the organization's problems be made public, should all its members be aware of its problems? Respondents said yes, mode and median equal to 4, range 4 and interquartile 1.5. The analysis of the mode and the median first show that, according to the agents, the existence of problems in the organization should be made publicly known to its members. As observed in the previous question, all agents answered this question, making it clear that the topic is relevant and needs to be made public.

Strategic planning must be supported by written procedures, and, if this information is to be preserved from the knowledge of a wider audience, a central concern is that this information does not reach competitors. The agents recognize that there are such procedures and concerns, presenting a mode and median of 5, range 3 and interquartile 1.

An ethical issue was raised in the survey regarding the agents' interest in sharing information about their past companies for the benefit of their new employer upon request. This issue includes a time limitation, less than two years after leaving the previous company. Mode and median equal to 1, that is, the agents disagree with this procedure, indicating that they would not provide such information in favor of the new organization in which they currently work. The range denotes dispersion equal to 4,

meaning that some respondents consider such sharing possible; what cannot be known is under what conditions these actors consider this position.

The development of new products or services requires planning, strategy in their launch and these preparatory phases must be handled with due care. Organizations make use of code names and nicknames to partially or totally remove the characteristics of a new project. Non-disclosure agreements (NDAs) are typically applied to vendors who will develop more sensitive parts of the new technology.

Yet there is a risk of information leakage insofar as the supply chain network is common among some industry segments, with some networks transcending territories as they are often made up of global suppliers. Agents were asked if the company should be careful when controlling and disclosing data about a new product to prevent information hacking.

The survey has shown that there is a mode classifying responses with a wide range of 5, while the median was 5, the range of 4 and interquartile 1. It can be concluded that agents recognize the importance of protective measures against information leakage, although a smaller portion is not aware or has partial knowledge about the practice of this measure. This characteristic became evident because only agents with L3 positions classified the absence or low presence of care with the preservation of information about the new products away from hackers´ actions.

Once it was known that information protection is important for a new project, agents were asked if such a practice exists at *Motores* and if care is taken in the area of sensitive information about new products in their development phase. The answers indicated the presence of a bi-modal reading with answers agreeing that there is a wide range of mode 5, and moderate coverage with mode 4, median 4, and range 3 because there is dispersion in the classifications obtained and an interquartile of 2. Another highlighted feature is the higher rate of non-respondents: the agents who reported not knowing the problem represent the majority (53.1%), therefore, they did not answer this question.

An unknown frontier appears here, which means that most respondents are not sure whether the organization has implemented protection measures against external attacks by hackers. The lack of knowledge about the existence or not of protective measures cannot lead us to conclude that there are no protective measures adopted by *Motores*, but it indicates that the theme may be restricted to a certain group, which would be feasible. Part of the respondents stated that there are protection measures against hackers, but another group states that the existing measures are fragile, or not very efficient. An opportunity to analyze this in more depth and evaluate existing measures may lead to an increase in their quality and verify the perception of whether such measures are really effective.

Knowledge protection can be achieved by using patents. This brings a competitive advantage as it prevents competitors from applying the solutions developed by the holder of such knowledge to similar products. At the same time there is a concern that the patent itself is a vehicle of knowledge disclosure. Some companies often choose simply not to register a patent believing that they are better protected; two classic examples being the Coca-Cola formula and the thermonuclear weapons cited in Galison (2004).

The question raised by the survey lies precisely at this point: do *Motores's* agents understand that a patent ensures protection against the copy of a product or technology by competitors? Answers lead to a mode of 5, median 4, range of 4, and interquartile of 2. Yes, mode and median ensure that agents believe that a patent ensures that

specific knowledge or product is not copied by competitors, but as in previous cases the range and inter-quartile have important dispersions. They indicate that there are even partially disagreeing views as to whether patents can provide a full guarantee of protection, as proven by the examples provided by Galison (2004).

Technological development can be obtained from resources, human resources, or also from using co-development or open development work. Agents were asked if they believed in self-development without using open developments such as open science. The views of respondents with mode 4, median 4, range 3 and interquartile 1 indicate that they believe in development with their own resources with a moderate degree of comprehensiveness, without sharing these needs to the academic community or others. The range dispersion was lower than those observed in previous questions suggesting a more conservative view when the theme involves joint developments, with internal resources and partnerships with the scientific community.

5. Research Findings Based on the Survey Data

Moreover, 30-60 minute long semi-structured interviews were conducted individually within the *Motores* work environment in a reserved room with 21 interviewees, in which there were L1 =6, L2 =6 and L3 = 8 people plus one respondent L3 who answered only the first two questions of the five valid ones. Answers whenever possible indicated the hierarchical level that expressed them. A summary is presented in Table 2 at the end of this section.

5.1 How do you understand confidentiality?

This was the first question asked in order to record the respondents' views and opinions on the subject. Confidentiality and its scope are understood to be strategic, tactical, and operational. A relationship of trust and complicity has to be established among the organization's members, Donaldson & Davis (1991); Porta et al. (1996)—an idea that has also been supported by Simmel (1906). The control of secrecy is its central point; if a leak occurs, secrecy no longer exists and the information kept secret becomes public knowledge, thereby losing its function. The element of control of confidentiality that is observed by agents in L2 is time.

In other words, confidentiality has a formal or informal expiration date that must be maintained before its objective can be achieved. A force that will imbue the process of maintaining confidentiality with trust rests with its members—actors with high maturity who can be classified as an asset of the organization according to L1. When it involves third parties, the issue of confidentiality has two relevant points in the opinion of L1. The first is the ability to maintain confidentiality without revealing the essentials to maintain opacity. For instance, the quoting process of certain products or components may have the character of a study of competitiveness, but in reality may hide the possibility of a takeover of a competing firm. The level of opacity is therefore subtle without leading to a lie.

The second point as a consequence of this opacity process is the tension generated in the administration of the work, since the background reason cannot be revealed. Confidentiality has the function of allowing a goal achievement, whether when carrying out a project, task, or mission, bringing about a competitive advantage and having the nature of an action to be taken. Sharing sensitive information is restricted;

organizational data, departmental information, and indicators leaving the associated control circle will pose problems for the organization if they reach competitors.

The agents expressed their views regarding the following points that should have their content undisclosed: salaries, poor professional performance, dismissal process, and behavior deviations such as theft, bribery, and participation in cartels. L3 added the following to this list: information leaks regardless of the hierarchical level, which may lead to serious consequences, including risks to the integrity of individuals or the business; the occurrence of information leakage about a new product before its patent application; or information about email layoffs that may suffer hacking actions. One option discussed was to make such announcements verbally, which goes back to the aforementioned, that is the idea that mature teams that will keep the information confidential within the control circle of the organization.

The action of leaking sensitive information to a competitor by the holder of that information will be understood as espionage, and actions of contention will be taken, including dismissal and lawsuits. The agents also regarded the existence of excess confidentiality in an organization to pose a risk of damage to creativity. They concluded by saying that secrecy is a difficult and sensitive asset to preserve, and the dismissal of the leak-causing agent is a way to close the issue insofar as the loss of confidence has occurred.

The comments from L1 were more oriented towards controlling information inside the control circle as cited by some interviewed agents:

> It is a consequence of company professionals. It is like a mirror of the grade of maturity of one organization. I earn more money than you - to whom it matters, without damaging the relationship. The other L1 agent highlighted the following: it is essential, within an organization, to achieve a goal without putting people and businesses at risk. Secrecy generates high tension when third parties need to be involved in the process. The secrecy is difficult (sensitive) to be preserved.

L2 and L3 reported that they are more focused on avoiding information leaks sensitive to competition. Some quotes that clarify this thought are as follows:

> The strategic plan of a new product, or strategic changes in these products, should not reach competitors´ ears; information is shared in parts, and the disclosure happens only with the agreement between the participants; something wrong happens such as a theft, cartel, and an investigation is carried out for a period. After the conclusions, the process is closed. In the case of the cartel, mysterious trips took place. Once concluded, part of the investigation can be revealed and others not. Dismissal is one way to terminate this subject as trust was lost. The organization is a home, some enter and others leave it; once trust has been lost, the relationship has to be ended.

Some body language during the interview of the first question could be observed, such as: when the agent heard the first question he was startled; a moment of reflection before answering it, visual communication, he asked if the interview would be about the work or a private topic.

5.2 Why does confidentiality exist?

The purpose of confidentiality, according to L1's opinion, is to safeguard strategies for developing future visions of the organization. There is a time function associated with the time required for a designated action to be started; it is the adequate time for a given action. Another perspective is that secrecy avoids conflicts of information among the different agents involved in a given process, thereby preventing distortions that can hinder workplace camaraderie, which is also mentioned in Donaldson & Davis (1991).

Agents also perceive sensitive events or sensitive information as determinants of stress and risk. For instance, a possible closure of a plant or product line or details of financial data should not be shared with the union. The flow of this and other similar information occurs in a filtered manner to mitigate risks and tensions in the lower echelons of the *Motores'* structure. Busnelo (2018) had an interesting view, comparing the German and Brazilian cultures and the exposure of people, which was reported by one of the agents:

In Brazil people's behavior is more opaque. When driving on a highway, for example, when we know the locations of speed cameras or when the police are imposing fines, we usually alert drivers who come in the opposite direction by flashing the vehicle's headlights, this is opacity. In Germany, I witnessed an accident on an Autobahn. Cars started to stop on the hard shoulder (some passing straight by). A driver closed the road and photographed the cars involved, called a witness and reported the police. He exposed the offending driver and revealed the violation.

The absorption of secrecy is a function of the degree of maturity. Some information leaks happen not due to bad faith but because of the lack of knowledge of the whole scenario — when the full scope of an issue and its possible consequences are lost (Busnelo, 2018). Other information leakage risks cited by Busnelo (2018) occur in the family environment, at the barber shop, country club, commemorative parties, church, as well as the already known corporate environments, class entities, government agencies, and the press.

Confidentiality does not exist only to preserve the strategy of the organization. Personal information and relationships within and outside the organization also require the preservation of confidentiality on private matters. Busnelo (2018) mentioned the veil of secrecy over homosexuality, for instance. Complicity and trust exist in situations of disclosure of private and particular problems. An individual's positive skills can be communicated after careful analysis of what information can be safely disclosed, but without revealing the main piece, whereas negative information should have restricted access, *arcanum.*

5.3 When should confidentiality be revealed, to whom, and why?

The disclosure of confidentiality only takes place with the consent of its owner, which in this study is the organization *Motores*. The extent of the scope and risk of such disclosure must be adequately assessed. Lawsuits or sharing of the know-how can cause immense damage to an organization.

Horn (2011) defined technical knowledge as eternal, *arcanum,* subject to controls on the access. According to Bobbio (2015), technocracy has its arcana or hidden rules. In cases involving specific projects, broader disclosures will be made available to its members. The criteria concerning whom to disclose to and by what means, in these

cases, are set by the organization. Disclosure is not necessarily only hierarchical according to L 1: functional influences and directions may cause the agents at a lower hierarchy to have access to confidential information when those above them do not.

Busnelo (2018) exemplifies this case by mentioning a project for the acquisition or incorporation of a company. Involvement of the financial and human resources departments mean that there will be a deeper level of analysis of contractual values and conditions, overlapping other executives of the organization who, despite being positioned hierarchically above in the structure, will not have direct access to such information, as they are not concerned with the functional areas involved. L2 understands that a disclosure about a new product can only occur if it is already protected by a patent, since sales and marketing strategies must be preserved forever, *arcanum*.

Disclosure should always be communicated when a benefit or risk reduction for the organization is detected. According to Costas & Grey (2014), the CEO of the organization shares the secret with his/her closest group, the *petit comité*. There is a divergence of points of view in the evaluation of L3 because for them the sharing of information and confidential disclosures must occur within a hierarchical structure in relation to the contradictory opinion of agent L1 above.

This leads us to reflect a little on this point. The disclosure of confidentiality may be both hierarchical and functionally hierarchical, as already mentioned. Both possibilities exist, with their form of disclosure and sharing being dependent on the nature of the issue or the project to be addressed. This study suggests that the more technical the theme, the greater the possibility of revelation that occurs within a functional hierarchical structure.

The act of disclosure must be preceded by authorization since there is an owner of the confidential information. The authorizing agent may be a person from the staff or an institution or the organization's proxy agent. The request for confidentiality or disclosure is usually made in a meeting behind closed doors, verbally in most cases, with a decision made within a specific context/period, with no written protocol (Busnelo, 2018).

Information can be disclosed both about negative and positive issues. Attempts should be made to clamp down on fake news that causes disturbances within the organization, involving suppliers, customers, and society. The correct version of the facts needs to be conveyed. Transparency, in this case, generates trust and credibility.

The L3 agents made some observations that confer the tension that exists when confidentiality must be preserved and disclose the hierarchical structure that resides in the *Motores* organization, as follows:

> Only reveal (something) when secrecy ceases to be so. Someone must authorize your disclosure. If I maintain confidentiality, I live in a shadow, maybe I decide to reveal it or not.

> There are different times for disclosure across the organizational structure L1 to L2 and from L2 to L3. It is direct from L1 to L2, in most cases. All based on the relationship of trust. How much the person can contribute with information (mentioning when a second person should be involved in confidentiality sharing, assessment phase). It is more gradual or evaluates whether you are able to help and understand. Gossip, if it turns out to be secret, confidential information without feedback, has no purpose, so it is gossip, free disclosure.

5.4 What should not be revealed and why not?

A risk analysis should be conducted before any information is disclosed, as the revelation can have positive or negative, tangible or intangible impacts on the organization's assets. The topics raised in L1 and classified as the most sensitive to a disclosure process concern financial issues, product strategy, technology - although valid in their purpose -, personal privacy and salary. Therefore, we have a condition that the content - salary value - is kept confidential and the effect, the promotion, is disclosed because it is public. We therefore have a condition in which the content—salary value—is kept confidential, and the effect, promotion, is disclosed because it is public.

The default rule for preserving confidentiality is that classified information should be disclosed down the organizational hierarchy. As one of the respondents in L1 explains, "people don't need one more worry on their shoulders." Going down the hierarchy will fulfill the purpose of the information, but an information triangulation should be conducted to ensure that the correct message has reached everyone.

Once more, organizational strategy emerges as an element that cannot be revealed in L2's view either. As a new product will be launched on the market, advanced studies on the frontier of knowledge, in this particular case, should never be revealed in advance, *arcanum*. Other issues face similar preservation concerns, not public knowledge, such as those related to environmental impacts or dismissal processes. For instance, a professional is dismissed while another is being hired in his/her place, thereby avoiding the bullwhip effect associated with hiring and firing.

The information of failures in projects need to be kept under the control of a restricted group, and only members of a particular group (by function and/or specific knowledge) should have access to such information, *arcanum*. This restricted committee, the *petit comité*, is the owner of the information, and the latter will remain within the group as a way of avoiding errors in future projects while preserving the know-how. Added to the list of non-disclosable information are the following: weaknesses in a product, as long as it does not involve the safety of people or of an asset; payroll records, kept in eternal secrecy, *arcanum*; personal conduct deviations; actors responsible for analyzing facts and complying with applicable sanctions.

L1, L2 and L3 agree that personal information must be preserved, while organizational information can be preserved or disclosed depending on the interests involved. Some phrases from the agents are revealed, as follows:

> There are things that cannot be revealed, they are dealt with by a select group, for example: relationships between people, capable professionals, but who have difficulty in relating to others. A change of role in the workplace can solve the problem. This will never be revealed, *arcanum*, that person, for example, speaks loudly, etc.

> Project failures must not be revealed in the organization world. The revealing can happen only for a restricted group, *petit comité*. In this case, the failure or error, is understood and kept in secrecy inside this *petit comité*.

> The process under analysis is not yet completely completed. Coca-Cola's secret is not revealed. Certain financial information should not be disclosed. You enter the system (would you disclose this to shareholders?). It is a paradox, referring to financial difficulties, for example.

> Providing for the dismissal of someone and, at the same time, the opening of a vacancy for the same position. It generates fragility, what do you believe in? Environmental impact issues at some levels, but they are not fully open. Avoid the whip effect.
>
> For the person or group when everything is resolved, clarify why it existed, what the purpose is to be revealed. But only when necessary, otherwise, it should not be. Confidentiality, when revealed, must bring a benefit, the evil must be kept in a box. Caution is necessary.
>
> Personal matters should not be disclosed, salary, personal relationship - inside and outside the workplace, people's financial situations, processes and products, inappropriate behavior. Technical knowledge will finally be discovered (Coca-Cola formula). Belief in blessing, when he or she transfers his secret to the other person, he or she no longer practices, otherwise the new person blessing will lose the power of healing.

Some body language during the interview of the fourth question could be observed, such as: thought, reflected before starting to answer it; thought before setting a compromising example.

5.5 Is transparency required? When or under what circumstances is it required?

Transparency is necessary and important when it affects the common good, which here is the condition of all the agents of the organization. It is fundamental and generates credibility. Special care should be taken while addressing issues that are sensitive for the organization and releasing such information to the public. Personal data, for instance, should be processed in a secure way, since this information belongs to the individual and not to the organization.

When disclosing information, the degree of maturity of the agent should also be taken into consideration, as expressed by L1. Testing events should be held, increasing or decreasing the degree of filters for some shared information according to the level of trust developed, with all cases being confirmed by control points.

Another way to reveal information is through the utilization of a “context”; it is a non-complete disclosure that can be used in many cases - a mirror replaced by opacity and a satisfied agent at the end of the process. In this passage, reference is made to a real case that occurred at *Motores*, when assessing the competitiveness of a competitor's product, which in fact hid the possibility of acquiring the competitor by *Motores*. The filters used in a disclosure process have a stabilizing function, which prevents members of the organization from drawing their own conclusions.

The agents regarded transparency to be hierarchical, filtered, translucent, and at times, opaque. Moreover, transparency should not be naïve as there is no transparency in the pure nature of the word. Once confidential information is revealed, there will be consequences, and these effects should be thoroughly evaluated before the disclosure process begins.

This study identified the following types of transparency processes at *Motores*: selective disclosure of information that the company considers favorable and NDAs. Confidentiality agreements allow for greater transparency in project development. The company has a L2 hierarchical level that acts on two fronts, which is a key element in

the process and in the subject of transparency insofar as actions such as the purchase of new items, new product or technology development strategies occur both in direct contact with suppliers and customers and within a network of confidentiality contracts.

An example of care in the transparency process could be identified in the disclosure of *Motores*' pricing policies to the market. This process was observed to have a lesser impact if future developments such as increase in prices and change in payment terms were only verbally disclosed. At first, disclosure was communicated in written form, in a document assuring competitors that future actions would be taken. When the process became verbal, the information became questionable in the eyes of the competitors, as there was no guarantee of such an action; only the words of the company. Another example can be found in the case of fatal accidents at work. Caution must be exercised. The memory of the deceased must be preserved, but a detailed study of the accident must be conducted, its cause must be determined, and measures to contain future risks of repetition should be taken—actions that can therefore become transparent and public.

L1, L2 and L3 agree that transparency is needed. On the other hand, L2 and L3 believe that some transparency must have filters, as a tool to protect the motivation of agents and mitigate tensions. The agents expressed this as follows:

> Transparency is important in the interfaces with customers, but it depends on the moment of the company. At the time of Nasdaq, it was reduced to corporate meetings. Filters have become more active. The filters have a protection function. Reduces false expectations, complaints ... conflict reduction.

> It's hard, man. Transparency is necessary, but it must be subdivided into hierarchical levels. There is transparency (which must remain) at the executive level, but it came to me and discouraged me, financial problems can also reach other levels. Knowing this, despite all the information I have, it is a risk to be here (talking about the risk of the company firing you). There should be a protocol on the extent of transparency in relation to the associated impact. Transparency is not a measurable thing. Difficult to contain, a leaked e-mail can be detrimental to an entire group.

> When information affects everyone's life, it is treated (filtered) because not everyone has the level of skill and competence to understand the context. It reaches all levels, when it is distorted, it´s a problem. The biggest problem for organizations is to think that everyone is homogeneous in understanding. If there are no filters, everyone draws their own conclusions and generates new messages, noise.

Some body language and testimony of agents at the end of the interviews:

See my hands sweating, moment of reflection before answering the question. It revealed a personal secret. In the parking lot he informed me that he thought more about this interview, about the subject of secrecy, saying he was worried, talked to his wife and mother-in-law at lunch. He thought about how secrecy can be taught, also concerned with succession in the company.

Pensive, reflective, he rubbed his hands, scratched his head. Concern shown after the interview, asking twice if the interview was useful.

He asked one of the agents interviewed why some people refused to answer the survey, the answer was: fear of exposing themselves.

Table 2. L1: Senior executive level; L2: Middle management level; L3 Low management level.

Secrecy knowledge	Area of influence	Actors (Agents) involved	Formalization level
Levels of knowledge concerning information confidentiality.	*Motores* departments.	L1, L2, L3.	Informal, only verbal when existent. No central rules detected. No mitigation plan exists.
Frontiers 1.	Related to competitor, class associations and government relationship.	L1, L2, L3.	Spheres where agents have less information or daily concerns. Contrary to spheres of suppliers and competitors.
Frontiers 2.	Organization data, agents, society.	L1, L2.	Information on preventing attacks by hackers is available at the top - L1 and L2. It is practically unknown at the L3 level.
Transparency.	Organization data.	L1, L2, L3 and L2, L3.	All agree that transparency is needed. On the other hand, L2 and L3 believe that some transparency should have filters as a tool of protection of agent motivation.
Code of ethics.	Organization and agents.	L1, L2, L3.	Agents do not intend to share information from their previous work in favor of the current employer. Despite this, due to the dispersion of responses, the result suggests that there is room for disclosure of some type of information. Not reached by research.
Secrecy control.	Organization.	L2.	Time is the element controlling confidentiality, observed by L2 agents. Confidentiality has a formal or informal validity period, and it must be met in order for its objective to be achieved. The understanding of secrecy is a function of the degree of maturity of its agents.
Confidentiality disclosure 1.	Agents.	L1 among others, depending on the case.	This may be hierarchical or functional hierarchical. Depending on the nature of the theme and the project to be addressed. The research suggests that the more technical the theme, the more likely its hierarchical structure. Increasing or decreasing of filters according to control points.
Confidentiality disclosure 2	Agents.	L1 among others, depending on the case.	Information can be revealed making use of “context”. It is a form of partial disclosure, transforming the mirror into an opaque version, leaving the agent satisfied at the end of the process.

Note: Authors´ own work.

6 Final remarks

This study has shown that intrinsic knowledge about the theme of secrecy exists, according to the respondents, and the following points can be highlighted:

There are different levels of knowledge concerning information confidentiality within *Motores*, indicating that there are areas where the subject is less developed and others

where it is more advanced. There is therefore no written standard that establishes both central rules regarding the subject of confidentiality and the mitigation measures to be implemented in the case of leakage.

There is a knowledge frontier in matters related to competitors, class entities and government, about which the interviewees have little or no knowledge, thus signaling an unknown area in the form and theme of the information at such levels of relationship.

On the other hand, the transparency of the organization's data must be total, which gives it a sense of trust, according to the agents' opinions.

Agents indicated that they would not share information regarding their previous organization in favor of their new position with a competitor; therefore, a code of ethics is signaled. However, there is an important dispersion in the opposite direction, which implies that something could be revealed under certain conditions. Unfortunately, however, such information lies beyond the scope of this research.

The responsibility of preserving the organization’s sensitive information against a hacker attack is concentrated at the highest management levels of L1 and L2. A frontier of the unknown emerges here: most respondents are unaware of whether the organization has implemented protection measures against external attacks from hackers.

Time is the element controlling confidentiality, as observed by L2 agents. Confidentiality has a formal or informal validity period, which must be met in order for its objective to be achieved.

Confidentiality permits the achievement of a goal, which may be carrying out a project, task, or mission, or putting the company in a position of competitive advantage; it has the nature of an action to be taken.

Some actions are more secure and can be protected against hackers if communicated verbally only between the agents involved. In the present study, the dismissal process has moved to this procedure.

The absorption of secrecy is a function of the degree of maturity. Some information leaks out not due to bad faith but because of the lack of knowledge of the whole situation. The notion of comprehensiveness of a theme and its possible consequences is lost (Busnelo, 2018).

How the notion of secrecy is understood depends on the level of maturity.

The criteria on who to disclose and by what means used in this event belong to the organization. Such revealing criteria are not necessarily hierarchical, according to the view of L1 agents, as they may have functional influences and orientations; lower hierarchical levels may have access to confidential information that is not accessed by higher level agents.

The disclosure of confidentiality may be hierarchical and may also be functional hierarchical. Both possibilities exist, and its form of disclosure and sharing will depend on the nature of the theme and the project to be addressed. This study suggests that the more technical the theme, the more likely it is that disclosure will take place within a functional hierarchical structure. The disclosure of information must also take into account the degree of maturity of an agent, which according to L1, must be tested against events, increasing or decreasing the degree of filters under certain shared information, as confidence increases. Confirmed by the control points.

Another way to reveal information is to use “context”. It is a form of disclosure that is not complete and can be used in many cases, leaving the mirror in opacity, as the agent leaving satisfied at the end of the process.

A study by Zucker et al. (1994) considered zones of influence in technological development near major universities in the USA. This work proved the existence of a correlation between the presence of great researchers in these universities and the technological development of the biotechnology industry. So-called spillovers have occurred, and knowledge has been disseminated in nearby areas, generating development, patents, and economic growth.

Unlike the study conducted by Zucker et al. (1994), the object of investigation in this research was to understand the views of *Motores'* agents with regards to classified information. Different levels of understanding procedures, concerns, information communication, its risks and consequences have been found.

This work, however, demonstrates that much remains to be studied, mainly about a topic that is very restricted to organizations. Some limitations found relate to the non-disclosure of the content of the topics addressed, or only a superficial discussion about them.

Suggested topics for further research include the following: investigating when and under what conditions agents understand that they can disclose information about their past companies in favor of their new organization; studying cases decided in court pertaining to cartel-making processes in the industry in a number of longitudinal segments; and assessing the progress made with changes in corporate governance laws.

The findings of this research contribute to a better understanding of a topic that needs a theory to explain it. This study highlights the need for written procedures, limits for sharing information and suggests that filters and opacity are also part of the toolkit that, if better systematized, guarantees the maintenance of confidentiality and its unfolding, the correct form of its disclosure, under the control of the responsible person, the owner, who, in this study, is the organization.

The lack of such procedures allows individual actions based on the best sense of experience of the organization's senior agents toward addressing sensitive issues that can sometimes cause significant harm to people, brands, and the society in which a business is embedded. Furthermore, they prevent mitigation actions from being taken in the event of leaks insofar as such measures are not known and in certain situations the recognition of the leak itself takes time or is not identified by the agents involved.

7 References

Arnott, D. C. (2007). Trust–current thinking and future research. *European Journal of Marketing*, 41(9/10), 981-987. http://dx.doi.org/10.1108/03090560710773291.

Barca, M. (2017). *Economic foundations of strategic management.* London: Routledge. http://dx.doi.org/10.4324/9781315257068.

Barney, J. B. (2006). *Gaining and sustaining competitive advantage.* Saddle River, New Jersey: Prentice-Hall.

Bertram, D. (2007). *Likert scales*. Retrieved in 2018, 12 June, from http://poincare.matf.bg.ac.rs/~kristina/topic-dane-likert.pdf.

Bobbio, N. (2015). *Democracia e segredo* (Org. Marco Revelli. Trad. Marco Aurélio Nogueira). São Paulo: Unesp.

Bok, S. (1989). *Secrets*: *On the ethics of concealment and revelation*. New York: Vintage Books.

Brasil. (2011, 30 de novembro). *Lei nº 12.529, de 30 de novembro de 2011. Dispõe sobre a Estrutura o Sistema Brasileiro de Defesa da Concorrência; dispõe sobre a prevenção e*

repressão às infrações contra a ordem econômica. Brasília, DF: Diário Oficial da República Federativa do Brasil. Retrieved in 2018, 12 June, from http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12529.

Bromiley, P. (2005). The behavioural foundations of strategic management. *The International Journal of Leadership in Public Services*, 1(1), 56-57. http://dx.doi.org/10.1108/17479886200500012.

Busnelo, H. C. (2018). *Confidentiality-multiple dimensions: Action of agents, forms of understanding and organizational dynamics*. São Carlos: Universidade Federal de São Carlos.

Busnelo, H. C., & Donadone, J. C. (2019). *Triad of secrecy in organizations: secret information understanding and boundaries that might impact on strategy*. Unpublished manuscript.

Capasso, A., & Dagnino, G. B. (2014). Beyond the “silo view” of strategic management and corporate governance: Evidence from Fiat, Telecom Italia and Unicredit. *The Journal of Management and Governance*, 18(4), 929-957. http://dx.doi.org/10.1007/s10997-012-9247-0.

Capasso, A., Dagnino, G. B., & Lanza, A., (Eds.). (2005). *Strategic capabilities and knowledge transfer within and between organizations*: *New perspectives from acquisitions, networks, learning and evolution*. Cheltenham, UK: Edward Elgar Publishing.

Charreaux, G., & Desbrières, P. (2001). Corporate governance: stakeholder value versus shareholder value. *The Journal of Management and Governance*, 5(2), 107-128. http://dx.doi.org/10.1023/A:1013060105433.

Coff, R. W. (1997). Human assets and management dilemmas: coping with hazards on the road to resource-based theory. *Academy of Management Review*, 22(2), 374-402. http://dx.doi.org/10.5465/amr.1997.9707154063.

Costas, J., & Grey, C. (2014). Bringing secrecy into the open: Towards a theorization of the social processes of organizational secrecy. *Organization Studies*, 35(10), 1423-1447. http://dx.doi.org/10.1177/0170840613515470.

Currall, S. C., & Inkpen, A. C. (2002). A multilevel approach to trust in joint ventures. *Journal of International Business Studies*, 33(3), 479-495. http://dx.doi.org/10.1057/palgrave.jibs.8491027.

Delerue, H., & Lejeune, A. (2011). Managerial secrecy and intellectual asset protection in SMEs: The role of institutional environment. *Journal of International Management*, 17(2), 130-142. http://dx.doi.org/10.1016/j.intman.2010.10.002.

Denis, D. K. (2001). Twenty-five years of corporate governance research… and counting. *Review of Financial Economics*, 10(3), 191-212. http://dx.doi.org/10.1016/S1058-3300(01)00037-4.

Derrida, J., Brault, P. A., & Naas, M. (1994). “To do justice to Freud”: The history of madness in the age of psychoanalysis. *Critical Inquiry*, 20(2), 227-266. http://dx.doi.org/10.1086/448710.

Diefenbach, T., & Sillince, J. A. (2011). Formal and informal hierarchy in different types of organization. *Organization Studies*, 32(11), 1515-1537. http://dx.doi.org/10.1177/0170840611421254.

Donaldson, L., & Davis, J. H. (1991). Stewardship theory or agency theory: CEO governance and shareholder returns. *Australian Journal of Management*, 16(1), 49-64. http://dx.doi.org/10.1177/031289629101600103.

Dufresne, R. L., & Offstein, E. H. (2008). On the virtues of secrecy in organizations. *Journal of Management Inquiry*, 17(2), 102-106. http://dx.doi.org/10.1177/1056492607313082.

Fama, E. F., & Jensen, M. C. (1983). Separation of ownership and control. *The Journal of Law & Economics*, 26(2), 301-325. http://dx.doi.org/10.1086/467037.

Ferrin, D. L., Dirks, K. T., & Shah, P. P. (2006). Direct and indirect effects of third-party relationships on interpersonal trust. *The Journal of Applied Psychology*, 91(4), 870-883. http://dx.doi.org/10.1037/0021-9010.91.4.870. PMid:16834511.

Friedman, D. D., Landes, W. M., & Posner, R. A. (1991). Some economics of trade secret law. *The Journal of Economic Perspectives*, 5(1), 61-72. http://dx.doi.org/10.1257/jep.5.1.61.

G1 14 ago 2008. Petrobras divulga nota sobre furto de dados. from http://g1.globo.com/Noticias/Economia_Negocios/0,MUL299212-9356,00-PETROBRAS+DIVULGA+NOTA+SOBRE+FURTO+DE+DADOS.html.

Galison, P. (2004). Removing knowledge. *Critical Inquiry*, 31(1), 229-243. http://nrs.harvard.edu/urn-3:HUL.InstRepros:2580255.

Goffman, E. (1978). The presentation of self in everyday life (p. 56). London: Harmondsworth.

Goffman, E. (2009). *Stigma: notes on the management of spoiled identity.* New York: Simon & Schuster.

Grandori, A., & Soda, G. (1995). Inter-firm networks: antecedents, mechanisms and forms. *Organization Studies*, 16(2), 183-214. http://dx.doi.org/10.1177/017084069501600201.

Granovetter, M. (1985). Economic Action and Social Structure: The problem of embeddednes. *AJS*, 91(3), 481-510.

Grey, C., & Costas, J. (2016). *Secrecy at work: The hidden architecture of organizational life.* Stanford, CA: Stanford University Press. http://dx.doi.org/10.1515/9780804798167.

Habermas, J., & Habermas, J. (1991). *The structural transformation of the public sphere: An inquiry into a category of bourgeois society.* Cambridge, MA: MIT press.

Hannah, D. R. (2007). An examination of the factors that influence whether newcomers protect or share secrets of their former employers. *Journal of Management Studies*, 44(4), 465-487. http://dx.doi.org/10.1111/j.1467-6486.2007.00694.x.

Harrigan, K. R. (2003). *Declining demand, divestiture, and corporate strategy*. Washington D.C.: Beard Books.

Hart, O., & Moore, J. (1990). Property rights and the nature of the firm. *Journal of Political Economy*, 98(6), 1119-1158. http://dx.doi.org/10.1086/261729.

Horn, E. (2011). Logics of political secrecy. *Theory, Culture & Society*, 28(7-8), 103-122. http://dx.doi.org/10.1177/0263276411424583.

Hoskisson, R. E., Cannella, A. A. Jr, Tihanyi, L., & Faraci, R. (2004). Asset restructuring and business group affiliation in French civil law countries. *Strategic Management Journal*, 25(6), 525-539. http://dx.doi.org/10.1002/smj.394.

Jensen, M. C. (2002). Value maximization, stakeholder theory, and the corporate objective function. *Business Ethics Quarterly*, 12(2), 235-256. http://dx.doi.org/10.2307/3857812.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305-360. http://dx.doi.org/10.1016/0304-405X(76)90026-X.

Jensen, M. C., & Warner, J. B. (1988). The distribution of power among corporate managers, shareholders, and directors. *Journal of Financial Economics*, 20, 3-24. http://dx.doi.org/10.1016/0304-405X(88)90038-4.

Kroeger, F. (2012). Trusting organizations: the institutionalization of trust in interorganizational relationships. *Organization*, 19(6), 743-763. http://dx.doi.org/10.1177/1350508411420900.

Ku, A. S. (1998). Boundary politics in the public sphere: Openness, secrecy, and leak. *Sociological Theory*, 16(2), 172-192. http://dx.doi.org/10.1111/0735-2751.00049.

Lafer, C. (2011). Vazamentos, sigilo, diplomacia: a propósito do significado do WikiLeaks. *Política Externa*, 19(04), 11-17.

Maccarthy, B. L., & Fernandes, F. C. (2000). A multi-dimensional classification of production systems for the design and selection of production planning and control systems.

Production Planning and Control, 11(5), 481-496. http://dx.doi.org/10.1080/09537280050051988.

March, J. G., & Simon, H. A. (1958). *Organizations.* New York: Willey

March, J. G., Schulz, M., & Zhou, X. (2000). *The dynamics of rules: Change in written organizational codes.* Stanford, CA: Stanford University Press.

<edb>Marin, L. (1998). The logic of the secret. In L. Marin. *Cross readings* (pp. 195-204, trans J.M. Todd). Atlantic Highlands, NJ: Humanities.</edb>

Porta, R. L., Lopez-De-Silane, F., Shleifer, A., & Vishny, R. W. (1996). *Trust in large organizations* (NBER Working Paper, No. w5864). Rochester, NY: National Bureau of Economic Research.

Porter, M. E. (2008). *Competitive advantage*: creating and sustaining superior performance. New York: Free Press.

Rao, A., & Schmidt, S. M. (1998). A behavioral perspective on negotiating international alliance. *Journal of International Business Studies*, 29(4), 665-694. http://dx.doi.org/10.1057/palgrave.jibs.8490047.

Roe, E. (1994). *Narrative policy analysis.* Durham, NC: Duke University Press.

Rumelt, R. P., Schendel, D. E., & Teece, D. J. (Ed.). (1995). *Fundamental issues in strategy: A research agenda*. News Brunswick, NJ: Rutgers University Press.

Simmel, G. (1906). The sociology of secrecy and of secret societies. *American Journal of Sociology*, 11(4), 441-498. http://dx.doi.org/10.1086/211418.

Stohl, C., & Stohl, M. (2011). Secret agencies: the communicative constitution of a clandestine organization. *Organization Studies*, 32(9), 1197-1215. http://dx.doi.org/10.1177/0170840611410839.

Teece, D. J. (1988). *Contributions and impediments of economic analysis to the study of strategic management*. Berkeley: University of California, Berkeley Business School.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509-533. http://dx.doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z.

The Economist 10 ago. 2013. The Snowden effect. Retrieved in 2017, 05 Aug, from https://www.economist.com/blogs/democracyinamerica/2013/08/american-surveillance

Thompson, E. D., & Kaarst-Brown, M. L. (2005). Sensitive information: a review and research agenda. *Journal of the American Society for Information Science and Technology*, 56(3), 245-257. http://dx.doi.org/10.1002/asi.20121.

Vermeir, K., & Margócsy, D. (2012). States of secrecy: An introduction. *British Journal for the History of Science*, 45(2), 153-164. http://dx.doi.org/10.1017/S0007087412000052.

Warren, S. D., & Brandeis, L. D. (1890). Right to privacy. *Harvard Law Review*, 4(5), 193. http://dx.doi.org/10.2307/1321160.

Weber, M. (2013). *Ensaios de Sociologia* (Trad. Waltensir Dutra, Revisão técnica: Fernando Henrique Cardoso, 5. ed.). Rio de Janeiro: LTC Editora. Retrieved in 2017, 05 Aug, from https://edisciplinas.usp.br/pluginfile.php/3952424/mod_resource/content/1/Max%20Weber%20-%20Ensaios%20de%20Sociologia%20-%20Gerth%20%20Mills.pdf–

Williamson, O. E. (1984). *Corporate Governance* (Faculty Scholarship Series, Paper 4392). Yale: Yale law journal.

Yin, R. K. (2009). *Case study research*: *Design and methods (applied social research methods)*. London and Singapore: Sage.

Yu, R., & Weise, E. (2017, May 15). Hackers demand ransom for stolen Disney movie. *USA today*. Retrieved in 2017, 05 Sept, from https://www.usatoday.com/story/money/2017/05/15/reports-hackers-demand-ransom-stolen-disney-movie/101726832/

Zaheer, A., & Harris, J. (2006). Interorganizational Trust. In O. Shenkar & J. Reuer (Eds.), *Handbook of strategic Alliances* (pp. 169-98). London: Sage. http://dx.doi.org/10.4135/9781452231075.n10.

Zerubavel, E. (2006). *The elephant in the room: silence and denial in everyday life*. Oxford University Press. http://dx.doi.org/10.1093/acprof:oso/9780195187175.001.0001.

Zucker, L. G., Darby, M. R., & Brewer, M. B. (1994). *Intellectual capital and the birth of US biotechnology enterprises* (Working Paper, No. 4653). Cambridge, MA: National Bureau of Economic Research.